



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,617	08/17/2000	David Platt	TIVO0043	6921

7590 11/18/2004

TiVo Inc.
2160 Gold Street
P.O. Box 2160
Alviso, CA 95002

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/642,617	Applicant(s) PLATT, DAVID	
	Examiner Pramila Parthasarathy	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to request for reconsideration filed on July 09, 2004. Original application contained Claims 1 – 26. Applicant has amended Claims 1, 4 – 14 and 17 – 26. No Claims were cancelled. New Claims 27 and 28 are added. Therefore, presently pending claims are 1 – 28.

Response to Arguments

2. Applicant's arguments filed on July 09, 2004, have been fully considered but they are not persuasive for the following reasons:

Regarding independent claim 1 and 14, applicant argued that the cited prior art (CPA) [Poisner U.S. Patent 6,108,785] does not teach or disclose, "a system that generates a response value using a lock value at said second party and wherein said lock value indicates a desired access mode". This argument is not found persuasive. Poisner clearly teaches a method and/or system to prevent unauthorized use of a device, including generating a response value using a lock value to assert a signal to disable the device if the response does not correspond to an expected response (Summary of the invention; Column 1 lines 56 – 65) and Poisner discloses generating a challenge value at first party (Column 1 lines 56 – 65; Column 2 lines 14 – 18 and Column 5 lines 12 – 47); transmitting said challenge to second party (Column 1 lines 56

Art Unit: 2136

– 65; Column 2 lines 14 – 18 and Column 5 lines 12 – 47); generating a response value using a lock value at said second party, wherein said lock value indicates a desired access mode (Column 1 lines 56 – 65; Column 2 lines 14 – 18; Column 3 lines 56 – 65; Column 4 lines 9 – 31 and Column 5 lines 12 – 47); transmitting said response value to said first party (Column 1 lines 56 – 65; Column 2 lines 14 – 18; Column 3 lines 48 – 65 and Column 5 lines 12 – 47) and validating said response value by said first party (Column 1 lines 56 – 65; Column 3 lines 48 – 65; Column 4 lines 3 – 7 and Column 5 lines 12 – 47).

As for new added Claims 27 and 28, Poisner discloses validating said response value further includes unlocking the disk drive in accordance with the desired access mode indicated by the lock value if the response value is valid (Column 4 lines 9 – 31 and Column 5 lines 12 – 47).

Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1 and 14. Dependent claims 2 – 28 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1 – 28 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 1, 5, 6, 9, 10, 14, 18, 19, 22, 23 and 28 are rejected under 35 U.S.C. 102(b) as being anticipated by Poisner (U.S. Patent No: 6,108,785).

Regarding Claim 1, Poisner teaches and describes a method for providing access between a first party and a second party (Column 1 lines 56 – 65), said method comprising the steps of:

generating a challenge value at said first party (Column 2 lines 14 – 18 and Column 5 lines 12 – 47);

transmitting said challenge to said second party (Column 2 lines 14 – 18 and Column 5 lines 12 – 47);

generating a response value using a lock value at said second party, wherein said lock value indicates a desired access mode (Column 2 lines 14 – 18; Column 3 lines 56 – 65; Column 4 lines 9 – 31 and Column 5 lines 12 – 47);

transmitting said response value to said first party (Column 2 lines 14 – 18;
Column 3 lines 48 – 65 and Column 5 lines 12 – 47); and
validating said response value by said first party (Column 3 lines 48 – 65;
Column 4 lines 3 – 7 and Column 5 lines 12 – 47).

Regarding Claim 14, Poisner teaches and describes an apparatus for providing
access between a first party and a second party (Column 1 lines 56 – 65), said
apparatus comprising:

means for generating a challenge value at said first party (Column 2 lines 14 – 18
and Column 5 lines 12 – 47);

means for transmitting said challenge to said second party (Column 2 lines 14 –
18 and Column 5 lines 12 – 47);

means for generating a response value using a lock value at said second party;
wherein said lock value indicates a desired access mode (Column 2 lines 14 – 18;
Column 3 lines 56 – 65; Column 4 lines 9 – 31 and Column 5 lines 12 – 47);

means for transmitting said response value to said first party (Column 2 lines 14
– 18; Column 3 lines 48 – 65 and Column 5 lines 12 – 47); and

means for validating said response value by said first party (Column 3 lines 48 –
65; Column 4 lines 3 – 7 and Column 5 lines 12 – 47).

Claims 5 and 18 are rejected as applied above in rejecting claims 1 and 14.
Furthermore, Poisner teaches and describes a method for providing access between a

first party and a second party, further including randomly generating said challenge value (Column 3 lines 61 – 67).

Claims 6 and 19 are rejected as applied above in rejecting claims 1 and 14. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, further including using a disk drive controller to generate said challenge value (Fig.1 #165, Column 4 lines 60 – 65).

Claims 9 and 22 are rejected as applied above in rejecting claims 1 and 14. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of using a cryptography circuit to generate said response value (Column 4 lines 9 – 26).

Claim 28 is rejected as applied above in rejecting claim 1. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes unlocking the disk drive in accordance with the desired access mode indicated by the lock value if the response value is valid (Column 4 lines 9 – 31 and Column 5 lines 12 – 47).

Claims 10 and 23 are rejected as applied above in rejecting claims 9 and 22. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value further includes the step of using an algorithm to generate said response value (Poisner Column 3 lines 42 – 61).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 2, 3, 15, 16 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (U S Patent 5,596,739) in view of Bensimon et al. (U S. Patent No. 5,533,125).

Claims 2 and 15 are rejected as applied above in rejecting claims 1 and 14. Furthermore, Poisner teaches and describes a method for providing access between a

Art Unit: 2136

first party and a second party, wherein said first party is a disk drive and said second party is a key device (Poisner Fig.1 #180, #120, #170, #140, Column 2 lines 66 – Column 3 line 6 and Lines 42 – 58 and Column 5 lines 12 – 47). Poisner does not explicitly teach a method for providing access between a first party and a second party, wherein said first party is a disk drive and said second party is a host computer. However Bensimon discloses providing access between a first party and a second party, wherein said first party is a disk drive and a second party is a host computer (Bensimon Column 2 lines 63 – Column 3 line 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner and Bensimon to prevent unauthorized use of a disk drive as taught by Poisner and Bensimon by the host computer as taught by Bensimon. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system.

Claims 3 and 16 are rejected as applied above in rejecting claims 2 and 15. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party (Column 1 lines 56 – 65), wherein said disk drive is locked when not accessed (Column 4 lines 3 – 31 and Column 5 lines 16 – 39).

Claim 27 is rejected as applied above in rejecting claim 15. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes unlocking the disk drive in accordance with the desired access mode indicated by the lock value if the response value is valid (Column 4 lines 9 – 31 and Column 5 lines 12 – 47).

5. Claims 4, 7, 8, 11 – 13, 17, 20, 21 and 24 – 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (U S Patent 5,596,739, hereinafter "Poisner") in view of Bensimon et al. (U S. Patent No. 5,533,125) and further in view of Van Oorschot et al. (U S. Patent No. 5,850,443).

Claims 4 and 17 are rejected as applied above in rejecting claims 3 and 16. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said challenge value and said lock value further includes the step of using logic to generate input data by applying complex algorithm (Poisner Column 3 lines 61 – 67). Bensimon discloses the disk drive to include a password security feature at the device level in that the disk drive cannot be used in any computer system unless the thief also knows the password (Bensimon Column 4 lines 45 – 56). Even when taken together, Poisner and Bensimon do not disclose using 512 bits for said challenge value and using 512 bits for said lock value. However, Van Oorschot discloses a method and a system for establishing shared

Art Unit: 2136

secret keys to allow authentication between two parties and the advantages of using 512 bits for said challenge value and using 512 bits for lock value (Van Oorschot Column 5 lines 60 – Column 6 line 55 and Column 7 lines 20 – 36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and using 512 bits for challenge value and lock value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claims 7 and 20 are rejected as applied above in rejecting claims 1 and 14. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said response value (Poisner Column 4 lines 9 – 16). Van Oorschot discloses using an exclusive OR (XOR) to combine the said challenge and said lock value (Van Oorschot Column 6 lines 56 – 60 and Column 7 lines 1 – 19). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and using an exclusive OR (XOR) to combine the said challenge and

said lock value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claims 8 and 21 are rejected as applied above in rejecting claims 1 and 14. Furthermore, Van Oorschot teaches and describes a method for providing access between a first party and a second party, wherein said step of generating said response value further includes using 160 bits for said response value (Van Oorschot Column 6 lines 50 – 55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and using 160 bits for said response value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claims 11 and 24 are rejected as applied above in rejecting claims 6 and 19. Furthermore, Van Oorschot teaches and describes a method for providing access between a first party and a second party, wherein said step of generating a said

response value further includes using a secure hash algorithm to generate said response value (Van Oorschot Column 6 lines 49 – 55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a method for providing access between a disk drive and a host computer by combining the teachings of Poisner, Bensimon and Van Oorschot to prevent unauthorized use of a disk drive as taught by Poisner and using a secure hash algorithm to generate said response value as taught by Van Oorschot. The motivation would have been to prevent the computer system from reading from, or writing to, the disk drive without matching the challenge value from the disk drive to the response value from the computer system and to prevent determination of the algorithm by unauthorized users.

Claims 12 and 25 are rejected as applied above in rejecting claims 11 and 24. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes wherein said disk drive controller receives the challenge and lock value (Poisner Column 3 lines 60 –67). Van Oorschot discloses computing a duplicate response value on said disk drive controller by performing a duplicate secure hash algorithm and comparing said response value to said duplicate response value (Van Oorschot Column 6 lines 49 – 55).

Claims 13 and 26 are rejected as applied above in rejecting claims 12 and 25. Furthermore, Poisner teaches and describes a method for providing access between a first party and a second party, wherein said step of validating said response value further includes unlocking the disk drive in accordance with the desired access mode indicating by the lock value if the response and duplicate response values match (Poisner Column 3 line 65 – Column 4 line 25, Column 5 lines 12 – 37 and Column 6 lines 20 – 40).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Angelo (U.S. Patent Number 5,887,131) Method for controlling access to a computer system by utilizing an external device containing a hash value representation of a user password.

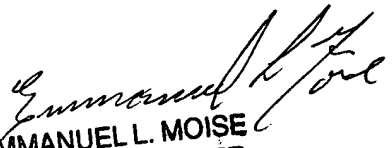
Diamant et al. (U.S. Patent Number 6,268,789) Information security method and apparatus.

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
November 13, 2004.


EMMANUEL L. MOISE
PRIMARY EXAMINER